10/564738
IAP15 Rec'd PCT/PTO 19 JAN 2006

SYSTEM AND METHOD FOR DETECTION AND LOCATION OF ROGUE WIRELESS ACCESS USERS IN A COMPUTER NETWORK

Field of the Invention

[0001] The present invention relates to methods to computer networks.

[0002] In particular, this invention relates to a method to detect and locate a rogue wireless access user to a computer network.

Background of the Invention

[0003] Wireless computer networks have grown in recent years not only for business enterprise environments but also for the small office / home office, universities and even cafes. The wireless local area networks (WLAN) make it very convenient for users to access information in a computer network, whether for work or recreation.

[0004] A WLAN makes use of wireless access points (AP) to send and receive signals to connect computers wirelessly to a central computer or server. Organizations provide WLANs to facilitate their employees, business partners, students or customers to access their servers.

[0005] However, unlike a wired local area network (LAN) where access means that a user's computer has to be physically connected to a network socket via a wire or cable, access to wireless LANs only require a user to have a wireless access card on his computer for access to the network.

[0006] This wireless access card may also be present as an in-built capability in computers and other wireless computing devices such as personal digital assistants (PDAs), tablet computers, mobile telephones and combination devices with features of these wireless computing devices.

[0007] In a WLAN deployment, while servers and access points have native security measures, these may not be sufficiently or properly enabled due to

ignorance, or are intentionally circumvented by users who desire faster access to the network.

[0008] Numerous methods and devices to restrict access to a WLAN to authorized users only abound. However, when an unauthorized or rogue user is detected, existing methods and devices of the prior art are not able to detect the geographical location of these rogue users.

[0009] To detect rogue users, the techniques of the prior art may use a wireless monitoring device that stores Media Access Control (MAC) addresses of users to compare the device number of each access point used against a list of authorized APs. This information may be correlated to Received Signal Strength Indicator values so as to give an idea of the distance the rogue user is from an AP of the network. However, determining and geographically locating the AP in question more precisely is not possible with the methods of the prior art.

[0010] To locate any rogue users in the network, a person has to use another device, a customized receiver with a directional antenna. This device is brought to the area where the rogue user is suspected to be in, to "home in" on his signals. Such a device may be couple to a Global Positioning System device as is taught by WO02/089507 (Younis).

[0011] Another invention uses a time acquisition unit to determine the distance of a mobile terminal from an AP (WO03/046600, Dietrich and Kraemer). Yet another invention (US2003023876, Bardsley), correlates network and intrusion information to find the physical connection port into the protected device rather than the geographical location of the rogue user.

[0012] However, all these inventions cannot detect and locate the rogue user without having to physically be on the ground, in the area covered by the WLAN. As such, these methods of the prior art are limited by requiring a human to physically patrol the area with a receiver to locate rogue users. Therefore, a method of detecting and determining the geographical location of unauthorized or rogue access users without having to be physically on the ground, will add an extra layer of protection to critical network resources

without having to incur high costs, especially in human resources. Such an invention will be welcome to address this deficiency in the prior art.

Summary of the Invention

[0013] The present invention seeks to provide a system and method against unauthorized, rogue users of a computer system.

[0014] Accordingly, in one aspect, the present invention provides a method to detect and geographically locate a rogue user wirelessly accessing a computer network, the method comprising:

deploying at least one Network Management System program;

mapping a geographical area covered by the wireless computer network into at least one island;

measuring at least one network performance parameter for each island to obtain a spatial performance model;

deriving a performance index for each island based on the at least one performance parameter;

identifying a potential rogue user based at least on his Media Access Control (MAC) address and Internet Protocol (IP) address;

measuring at least one performance parameter of the potential rogue user;

deriving at least one performance index for the potential rogue user;

determining location of the potential rogue user by comparing the performance index of the potential rogue user with historical, average performance indices of each island pertinent to the current time of detection; and effecting at least one network security measure against the rogue user.

[0015] In another aspect, the present invention provides a system to detect and geographically locate a rogue user wirelessly accessing a computer network, the system comprising:

a computer network with at least one wireless access point,

at least one processor,

at least a network management system,

at least one storage means, and

at least one implementation of the algorithm of the present invention, wherein the rogue user is able to be geographically located without having the computer network's user having to be physically in the vicinity of the rogue user.

Brief Description of the Drawings

[0016] A preferred embodiment of the present invention will now be more fully described, by way of example, with reference to the drawings of which:

[0017] FIG. 1 is the overall flowchart of how the present invention works.

[0018] FIG. 2 shows the islands around a wireless access point with similar network performance characteristics.

[0019] FIG. 3 is a more detailed flowchart showing how the algorithm of the present invention works in one embodiment of the invention.

[0020] FIG. 4 is a more detailed flowchart showing how the algorithm of the present invention works in another embodiment of the invention.

Detailed Description of the Drawings

[0021] The invention will now be described. In the following description, details are provided to describe the preferred embodiment. It shall be apparent to one skilled in the art, however, that the invention may be practiced without such details. Some of these details may not be described at length so as not to obscure the invention.

[0022] There are many advantages of the preferred embodiment of the invention. The advantages of the preferred embodiment include allowing the network administrators using the invention to monitor, detect and locate rogue users speedily in the wireless networks without leaving his desk. When a rogue user is detected, security measures may be taken against him. When repeat offenders are located after being warned, they may be prosecuted according to the applicable laws of the country concerned.

[0023] The present invention provides a method and a system using network performance information to detect and geographically locate rogue users in a wireless computer network.

[0024] The overall strategy of the present invention is illustrated in FIG. 1. First, a commercially-available Network Management System (NMS) is deployed **101** to establish the spatial performance model **102** for a WLAN. This is done by collecting and mapping out the performance characteristics of wireless computers in various spots or islands, identified by their respective position indices (eg **1, 2, 3, 4, 5,** etc in FIG. 2), in the area covered by the wireless access points (APs) of that network. This area is typically in buildings and the surrounding areas where genuine, authorized users may log on wirelessly into the network, and where rogue users may intermingle and hide in plain sight while connecting to the WLAN. Also of interest will be hidden areas such as blind corners and stairwells where rogue users may favour.

[0025] The mapping may be ad hoc, that is, as and when users log on in various known, pre-identified, areas for wireless access such as a dedicated lounge for "hot desking" workers or university cafeteria with APs for students. Alternatively, the mapping may be systematic, that is, a member of the information technology office staff may position himself at each pre-identified or predetermined island or spot, log on wirelessly with a computer or a suitable wireless computing device, and allow the performance characteristic of his computer or device to be captured for each spot or island.

[0026] Thereafter, the performance characteristic of each spot or island (as identified by their respective position index) may continually be captured and monitored at fixed intervals throughout the day. As such, this information is dynamically updated at these time intervals by the deployed Network Management System (NMS) used by the network. Under the present invention, the performance characteristic of each spot is the aggregate of the measured values of various network performance parameters for that spot or island. As the performance of the wireless network changes through the day depending on the number of users accessing the system, these spots or islands may also be dynamically

changed and updated, grouped according to substantially similar performance characteristics at each particular point in time.

[0027] The idea is, when a suspected rogue user is detected **103** based on his Media Access Control (MAC) and Internet Protocol (IP) addresses, an algorithm, an element of the present invention, may be used to locate him using the performance characteristic **104** of his computer at a spot which has been mapped to position indices **105** in the surrounding area.

[0028] A variety of security measures may then be taken, ranging from merely logging his particulars in an audit trail **106** or displaying his most probable location **107**, to preferentially denying him access the next time, to prosecuting him according the prevailing laws of that jurisdiction.

[0029] Thus, the spatial performance model of the present invention links the performance characteristic of each island with their location. In other words, the spatial performance model is used to identify the location of a rogue user by his computer's network performance characteristics.

[0030] To establish the spatial performance model for a particular WLAN, any suitable, commercially available NMS software may be deployed (**101**, FIG. 1) and used. These programs are able to collect and show the MAC and IP addresses of computers and access points logged into the network as well as other performance characteristics of each wireless connection to the network.

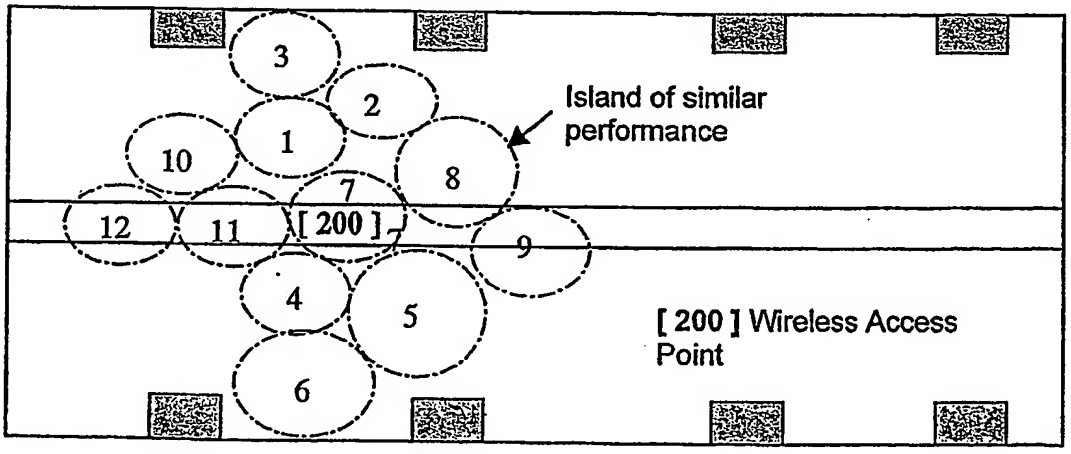
[0031] Each "layer" of the network system has performance parameters whose values varies in accordance with the following variables such as distance from access point, number of wireless users, network topology, building materials used, and time of day. These performance parameters may be used for the determination of geographical location of rogue user.

[0032] With reference to the Open System Interconnection (OSI) reference model for data communications, at the physical layer, the signal strength and signal-to-noise ratio may be used. At the network layer, "ping" response time and propagation delay times may be used. At the application layer level, the transaction response and delay times may be used. At the data link layer, the link utilization, packet rate, number of error packets and

throughput rate may be used as performance parameters. These parameters are merely examples of measurements that may be used and the present invention is of course not limited to use of only these parameters.

[0033] Now, as the distance of a user's computer from a wireless access point (AP) increases, the network performance pertaining to that user's computer decreases. Deterioration in network performance is also affected by building structures that reduce the transmission strength of the signals.

[0034] Thus, a unique map of the area of coverage by the WLAN may be plotted using at least one performance parameter or characteristic. The model may also be presented with the performance characteristics represented as a derived index value. Of course, the more parameters measured and represented, the better. This map is illustrative of the spatial performance model. The diagram below shows the various spots or islands around a wireless access point **200** identified by their respective position indices in the map sharing the same performance characteristics at a particular time period of the day (FIG. 2 and also below). It will be appreciated that this mapping of the islands or spots in the area covered may be dynamic and the mapping is updated as the performance characteristics of the islands or spots change.



[0035] This information may also be listed into a corresponding matrix table representing the spatial performance model (102, FIG. 1), an element of the present invention. The matrix table for the above diagram is:

Principal Direction	North			South			East			West		
Position Index, j	1	2	3	4	5	6	7	8	9	10	11	12
Ping Response Time	0.08	0.15	0.11	0.12	0.18	0.14	0.07	0.17	0.1	0.05	0.2	0.3
Signal To Noise Ratio	0.9	0.55	0.7	0.82	0.45	0.65	0.86	0.6	0.75	0.92	0.4	0.65

[0036] This table is logged and dynamically updated by the NMS periodically throughout the day, depending on the processor demands of the network and also on the possibility of the threat of rogue users. This periodic updating is performed as the performance characteristics vary with the number of users logging into the network. For example, the network characteristics may be optimal at the early hours of the morning and least optimal during the day when the network's wireless traffic is heaviest. These records are stored and averaged to obtain dynamic, moving averages for the performance characteristics of each spot or island at each time period of the day.

[0037] Under the present invention, the NMS may be readily configured to periodically collect MAC and IP addresses of users wirelessly connected to the system for identification of possible rogue users. The identification is done by comparing the collected MAC and IP addresses with a reference set of valid addresses of authorized users. Users with addresses not on this reference set are considered as potential rogue users **103**.

[0038] The next step in the method of the present invention is to analyse and geographically locate these potential rogue users. This step has two parts. First, the subnet address and hence, the nearest wireless access

point (AP), serving the rogue user is determined by performing a logical AND operation between the captured IP address and the subnet mask of the rogue user.

[0039] The second part is to refine and determine the geographical location of the rogue user with reference to this, the nearest AP. To do this, the performance characteristics of the potential rogue user are captured **104**. Then a ranking algorithm, an element of the present invention, is used to compare the performance characteristics of the potential rogue user with the average of the historical reference performance characteristics pertinent to the time of day of detection **105**.

[0040] The algorithm normalizes, ranks and yields a performance index, representing the performance characteristics of each island covered by the nearest AP, with that of the rogue user's. Appropriate actions may then be taken **106**, **107**.

[0041] This method of the present invention essentially locates geographically potential rogue users based on their performance characteristics which standout from the background of moving performance averages.

[0042] This setup of the method of the present invention may be implemented in a number of ways and two embodiments of mathematical operations are given to illustrate its application. In no way should the present invention be seen to be limited to these two examples as many other mathematical operations that achieve normalization and ranking of performance values to establish the closest fit may be used to implement this step of the method of the present invention.

[0043] The following example illustrates how the algorithm works by a first series of mathematical operations. The two performance parameters used, ping response time and signal to noise ratio, are only illustrative and do not limit the present invention.

[0044] Table 1 below shows the historical, average values, $P_{i,j}$ of the selected performance parameters of 12 islands around an access point for the time period in question **301**.

Principal Direction	North			South			East			West		
Position Index, j	1	2	3	4	5	6	7	8	9	10	11	12
Ping Response Time, $P_{1,j}$	0.08	0.15	0.11	0.12	0.18	0.14	0.07	0.17	0.1	0.05	0.2	0.3
Signal To Noise Ratio, $P_{2,j}$	0.9	0.55	0.7	0.82	0.45	0.65	0.86	0.6	0.75	0.92	0.4	0.65

Table 1

[0045] And the values of the performance parameters of the rogue access user captured at time of day, C_i **302** are :

Ping Response Time, C_1	0.07
Signal To Noise Ratio, C_2	0.88

[0046] Subtracting to obtain the differences $E_{i,j}$ for the values of each performance parameter, i at each position index, j **303** using the formula

$$E_{i,j} = |C_i - P_{i,j}|,$$

(where C_i is the captured performance parameters of rogue user at time of day, $P_{i,j}$ is the moving average of the performance parameters at each position index or island),

we get Table 2 below.

Principal Direction	North			South			East			West		
Position Index, j	1	2	3	4	5	6	7	8	9	10	11	12
$E_{1,j}$	0.01	0.08	0.04	0.05	0.11	0.07	0.01	0.1	0.03	0.02	0.13	0.23
$E_{2,j}$	0.02	0.33	0.18	0.06	0.43	0.23	0.02	0.28	0.13	0.04	0.48	0.23

Table 2

And the minimum values for each differences **304** are:

$E_{1\ min}$	0.01
$E_{2\ min}$	0.02

[0047] Normalizing the value of each differences to obtain the rank numbers, $R_{i,j}$ **305** using the formula

$$R_{i,j} = E_{i,j} \ / \ (E_{i,j})_{min},$$

(where $E_{i,j\ min}$ is the minimum for each difference), we get the rank numbers $R_{i,j}$ in Table 3:

Principal Direction	North			South			East			West		
Position Index, j	1	2	3	4	5	6	7	8	9	10	11	12
$R_{1,j}$	2	16	8	10	22	14	1	20	6	4	26	46
$R_{2,j}$	1	16.5	9	3	21.3	11.5	1	14	6.5	2	24	11.5
S_j	3	32.5	17	13	43.5	25.5	2	34	12.5	6	50	57.5

Table 3

[0048] Summing up the columns for each position index to obtain S, the sum of rank number for each position index, j **306** . Thus S is the derived performance index for each island as identified by their respective position indices. From the performance index S, we can obtain the island or spot with the lowest value, which is the most likely location of the rogue user **307**, where

$$S_j = \sum_{i=1}^{n} R_{i,j}$$

In this example, n = 2, since two performance parameters were selected.

[0049] To practice the invention, other series of mathematical operations may also be used as is illustrated by the following second method example. The data in Table 1 **401** is again used in this second example.

[0050] The values of the performance parameters are first normalized by dividing them with the smallest value for that parameter **403, 404.** (From Table 1, the smallest value of the parameter of ping response time is 0.05, and for the signal to noise ratio parameter, it is 0.4.)

[0051] The normalized values are given in Table 4:

Principal Direction	North			South			East			West		
Position Index, j	1	2	3	4	5	6	7	8	9	10	11	12
Ping Response Time, normalised $P_{1,j}$	1.6	3	2.2	2.4	3.6	2.8	1.3	3.4	2	1	4	6
Signal To Noise Ratio normalised $P_{2,j}$	2.25	1.38	1.75	2.05	1.13	1.63	2.15	1.5	1.88	2.3	1	1.63

Table 4

[0052] The captured performance parameters of rogue user, C_i are then divided by the smallest value **403** to obtain normalized values **405** as tabulated below:

Ping Response Time, normalised C_1	1.4
Signal To Noise Ratio, normalised C_2	2.2

[0053] The differences are calculated for each spot or island **406** by subtracting the normalized captured performance parameter value of rogue user and the normalized values of spatial performance model and these are

summed **407** to obtain the value of S, the performance index for each spot or island. The results are given in Table 5:

Principal Direction	North			South			East			West		
Position Index, j	1	2	3	4	5	6	7	8	9	10	11	12
$E_{1,j}^{\text{normalised}}$	0.2	1.6	0.8	1	2.2	1.4	0.1	2	0.6	0.4	2.6	4.6
$E_{2,j}^{\text{normalized}}$	0.05	0.83	0.45	0.15	1.08	0.58	0.05	0.7	0.33	0.1	1.2	0.58
S_j	0.25	2.43	1.25	1.15	3.28	1.98	0.15	2.7	0.93	0.5	3.8	5.18

Table 5

[0054] By this second method example, the most probable location of the rogue user is given by the island or spot with the smallest performance index (S value) **408**, which, in this case is location number (or position index) 7.

[0055] Thus, no matter the number of possible mathematical methods used for deriving the performance indices of the islands and that for rogue users, the same or substantially the same method is used to for both the islands and for the rogue users.

[0056] Upon determining the location by the methods of the present invention, immediate arrival at the spot or island by the network administration or law enforcement staff may allow photographic evidence of the intrusion as well as the likeness of the rogue user to be captured for identification purposes. The measures taken after detection and determination of the rogue user's geographical location of course depend on the prevailing laws of the land.

[0057] Thereafter, the location and performance characteristics of the rogue user may be recorded and flagged for tracking. In addition, predetermined security measures such as denial of access, warnings and prosecution may be effected according the user's organizational security and computer usage policies.

[0058] A person skilled in the art will appreciate that the method of the present invention is to first map the areas covered by the various wireless access point of the computer network. Thereafter, the network performance characteristics of each location spot sharing substantially the same characteristics, are determined by aggregating various network performance parameters to obtain background values and to establish the spatial performance model of the present invention. As shown by the examples given, this aggregation may be obtained by a number of mathematical operations which all yield the same objective: to derive a performance index that reveals the most probable geographical location of the rogue user.

[0059] In the techniques of the prior art, any rogue user accessing the network may be identified by his MAC and IP addresses. However, the spatial performance model of the present invention may then be used to locate him by matching the performance characteristics of his computer with that of the island or spot with the same or substantially the same performance characteristics.

[0060] The person skilled in the art will also recognise that the algorithm of the present invention may be readily represented by various equivalent mathematical operations and implemented in a variety of programming languages or routines, to be linked to the NMS so that the present invention may be implemented and practiced.

[0061] Thus, to enable the invention to be practiced, a person skilled in the art will appreciate the minimum physical embodiment of the present invention consists of a computer network with at least one wireless access point, at least one processor, at least a network management system, at least one storage means and at least one implementation of the algorithm of the present invention. By implementing the algorithm of the present system in such a computer network, rogue users may be located without having any of the network's staff having to be physically in the vicinity of the rogue user to locate him, unlike the limitations of the prior art. Other

variations and embodiments of the present invention will be under the present invention.

[0062] The present invention therefore provides a method, an algorithm and a system for detecting and geographically locating rogue access users to a wireless computer network that overcomes, or at least alleviates, the limitations of the prior art.

[0063] It will be appreciated that although one preferred embodiment has been described in detail, various modifications and improvements can be made by a person skilled in the art without departing from the scope of the present invention.